

REMARKS

Claims 1-5, 8, 12-15, 17, 22, 9-11, 24, 25, 29-30, 32-35, 49, and 50 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Rosen. Applicants respectfully traverse for at least the following reasons.

Applicants respectfully submit that Rosen does not teach or suggest a digital signature of digital data D_3 in respect of first or second digital data D_1 or D_2 as defined in claim 1. The Office Action states that first digital data D_1 is described in Rosen as a preview/advertisement of a merchandise ticket, as disclosed in col. 4, lines 33-39 and 45-50. Col. 4, lines 33-39 discloses that a merchant's trusted agent (MTA) sends electronic merchandise to the customer's trusted agent and in return the customer's money module sends electronic money through the merchant's money model. Lines 45-50 disclose that a ticket is an electronic item created by an MTA. One example of such a ticket is for encrypted electronic merchandise.

The Office Action further cites col. 5, line 59 through col. 6, line 1 as D_1 . This section of Rosen discloses a component section of a decryption ticket (for enclosing electronic merchandise) including an object identifier field, which uniquely identifies a particular electronic object and may also contain a short description. The Examiner states that this short description of the object identifier can be D_1 because it constitutes a preview of the ticket.

The Office Action generally cites the consumer's request for a ticket as second digital data D_2 . Particularly, the Office Action cites col. 4, lines 45-50, which discloses that

the ticket is an electronic item created by an MTA and transferred to a CTA during a purchase transaction, and that a customer who has just received a ticket may only use the ticket upon successful completion of the transaction. The Office Action also cites col. 4, lines 33-39 for D₂ in which the consumer is stated to request a ticket from a merchant.

The Office Action then concludes that the unique ticket issued to the consumer by the merchant represents D₃. Particularly, the Office Action cites col. 7, lines 30-38, which states that the issuer signature section of a ticket holds a digital signature from the ticket creator over the identifier component sections and the signature is made using a private key belonging to the issuer's trusted agent, and then the issued certificate contains a certification by a trusted third party used in conjunction with the issuer's signature to verify the authenticity of the ticket.

However, there is nothing in Rosen that discloses that this issuer signature, or what is signed to create the digital signature, is based on what the Office Action cites for D₁ or D₂. According to claim 1, third digital data D₃, which is signed by a private signature key, must be generated in respect of either D₁ or D₂. If D₁ is the object identifier field or the presentation of a potential ticket, Rosen fails to teach or suggest that this information is used to create a D₃ that is digitally signed using a private signature key. Also, information relating to a consumer's request for a ticket (stated to be D₂) is not stated to be used for digitally signed data D₃. Referring to col. 7, line 29, the digital signature formed by the ticket creator over the identifier and components section is unrelated to use of either the preview of the contents of an electronic object or the consumer's request for a ticket.

Another example cited in the Office Action for D_3 is col. 6, lines 7-8, which states that the object signature field creates a digital signature of the electronic object. But according to claim 1, the digital signature has to be of digital data D_3 , and D_1 or D_2 must be used in respect of generation of the digital signature of third digital data D_3 . The electronic object's digital signature is a completely different field of the ticket. Particularly, the electronic object and digital signature thereof are in section 44, whereas a component section 12 with an object identifier field 36 includes the short description or preview. There is nothing in Rosen that indicates the electronic object digitally signed in field 44 is generated by either the merchant's advertisement/presentation of a potential ticket to be purchased or the consumer's request for the ticket. There also is nothing in Rosen that states that the short description in the object identifier 36 is used to create the electronic object, let alone the digital signature 44. This is even assuming, only for the sake of argument, that the computer of the ticket provider includes the MTA or merchant's trusted authority.

Still further, Rosen does not specifically mention that digital data D_3 is recovered using a verification key. Instead, a digital signature is applied according to col. 6, lines 7-8 to check whether the electronic object has been altered. As to col. 25, also cited in the Office Action, this section teaches that a host checks to see whether a ticket is active, wherein the trusted agents establish a session and A checks B's merchant credential. However, this does not mention recovery of digital data D_3 . The issuer is not recovered from an issuer signature, and nothing in Rosen states the electronic object itself is recovered at this

time (it is decrypted instead by the separate decryption keys of the ticket). For at least these reasons, Applicants respectfully request reconsideration and withdrawal of the rejection.

Claim 2 is believed to be allowable for at least the reasons stated above regarding claim 1 plus additional reasons. Particularly, the Office Action cites col. 11, line 67 for second digital data D_2 . However, this citation is inconsistent with the Office Action's statements regarding claim 1, because D_2 as used in the rejection of claim 1 is purported to be the consumer's request for a ticket. Col. 11, line 67 is not related to a consumer's request for a ticket, but relates to validation of a trusted server certificate. Further, digital data D_2 , according to claim 1, must be a second communication from the ticket consumer to the ticket provider. This is not disclosed in Rosen regarding the validation of a trusted server certificate.

The Office Action also submits that the one-way function (hash) feature is met on col. 11, line 67, and the feature of calculating in the computer of the ticket provider where the third communicating is of $\text{Sign}(s, I \parallel \text{hash}(R))$ as the digital ticket is submitted to be taught at col. 11, lines 14-67 and col. 12, lines 1-15. However, these two sections are directed to certification of a trusted server and to a trusted agent, respectively. According to claim 2, $\text{hash}(R)$ must be sent from a ticket consumer to a ticket provider, and the ticket provider must produce the digital signature of $\text{hash}(R)$. In Rosen, the digital signature is made by either a primary trusted server for a trusted server, or by a trusted server for a trusted agent, during initialization. Both digital signatures (including hash functions) are of an ID number, a public key, and expiration data.

The Office Action states (paragraph 2) in response to Applicants' previous remarks that Rosen on col. 11, lines 31-67 and Fig. 6A show the functions that make up a trusted server. The Office Action further states that X is equivalent to $\text{cert}(\text{TS})$. However, X is clearly stated in col. 11, lines 46-50 to be equal to $\text{TS}(\text{id})\|\text{TS}(\text{PK})\|\text{expire data}$ (see the bracket clearly delineating X). $\text{TS}(\text{id})$ is a unique trusted server identification number (known and assigned by the PTS and TS, respectively), $\text{TS}(\text{PK})$ is a trusted server public key, and "expire data" is the date that the certification expires. These three pieces of data, not $\text{cert}(\text{TS})$, provide X. The Office Action states that because X is a function of the hash value it is a unique value to the merchant computer/ticket provider. However, X is not a function of the hash value, but instead the hash value is taken of X.

Further, the information described in the certification process is specifically stated to be performed only once, prior to distribution of the trusted agent to the public, and is performed between either a trusted server and trusted agent, or between a primary trusted server and a trusted server, not between different trusted agents. In other words, a CTA does not send data to an MTA for creation of the digital signature in cols. 11-12. This initialization data is not related to a preview of the ticket, stated by the Office Action to be D_1 , or the request by the consumer to buy the ticket, which is stated by the Office Action to be D_2 .

Additionally, claim 2 defines calculating in the computer of the ticket provider a digital signature in respect of the third digital data D_3 including the one-way function of $\text{hash}(R)$ plus information I concerning the event for which the ticket is had. According to

the cert(TS) and cert(TA) definitions, in col. 11, lines 46-49, E_{PTS} is an encryption of X with an encrypted hash of X. However, neither the trusted server ID, the trusted server public key, nor the expiration date of the certification, i.e., the components of X, relate to information concerning the event for which the ticket is had. Thus, this section of Rosen fails to teach or suggest at least this additional feature of claim 2.

The Office Action rejects claim 3, stating that the feature “wherein the determining still further proceeds so that if the read digital ticket is the first uniquely presented then the digital ticket is valid else if the read digital ticket is not the first uniquely presented then the digital ticket is invalid” is found at col. 12, lines 15-18. However, this section relates to a trusted agency, recertification of the trusted agents and servers by the trusted agency, and providing untrusted lists and updated public key lists. None of these are related to a particular digital ticket, let alone to what the Office Action cites as D_1 and D_2 .

Claim 4 defines at least that the second communicating is of a one-way hash function $\text{hash}(R)$ of a number R and the calculating in the computer of the ticket provider is of a digital signature in respect of signature key s of $\text{hash}(R)$ and I. According to claim 4, the second communicating must be from the ticket consumer to the ticket provider. However, the hash function described in Rosen, col. 11, lines 14-67 and col. 12, lines 1-15 is between either a merchant computer and a merchant trusted agent, between the merchant trusted agent and a trusted server, or between a consumer trusted agent and a trusted server. None of these communications are between a consumer (or consumer trusted agent) and a merchant (or

merchant trusted agent). Therefore, the second communicating in claim 4 is not disclosed in Rosen.

Further, claim 4 defines that the calculating the computer of the ticket provider is of a digital signature in respect of hash(R) plus information I. Again, since all communication in col. 11, line 14 through col. 12, line 15 is between either an individual trusted agent and a trusted server, or between a computer or merchant and its respective trusted agent, the cited section of Rosen fails to teach such communication and calculation of digital signatures between the merchant and the consumer. Applicants respectfully submit that claims 5-7 are allowable for at least the reasons stated above regarding claims 1-4.

As to claim 8, Applicants respectfully submit that the Office Action rejection includes citations that cannot be combined to teach all of the claimed features. For example, the Office Action states that the feature of a ticket consumer deciding to obtain a ticket is met on col. 4, lines 33-39, 45-50, which discloses that trusted agents exchange electronic merchandise and payment and that a ticket is an electronic item. However, the Office Action also submits that disclosure of the feature wherein the first calculating in the computer of the ticket consumer is a number R and the second calculating in the computer ticket consumer is a one-way function of the number R as hash(R) is met on col. 12, lines 1-15. This latter section is directed to the validation of the certificate of a trusted agency, not with the prospective ticket consumer deciding to obtain a ticket for a particular selected event and thus to become a ticket consumer, and not with the teachings of col. 4. lines 33-39 and 45-50.

Further, Claim 8 defines at least that the first calculating is in the computer of the consumer (the number R), the second calculating is in the computer of the ticket consumer (hash(R)), and the third calculating is in the computer of the ticket provider (to create $\text{Sign}(s, I || \text{hash}(R))$). Again, nothing in Rosen states that the portions of a digital signature of hash(R) are created in the ticket consumer and the ticket provider in this defined manner. Instead, the hash function and encryption described is for certification of a trusted agent or certification of a trusted server.

More particularly, there is nothing in Rosen that describes calculating in the computer of a ticket consumer (either a customer or a CTA), a number R, calculating in the computer of the same ticket consumer a one-way function of the number R as hash(R), sending hash(R) as a second communication to the ticket provider (merchant or MTA), and the ticket provider digitally signing D_3 including hash(R). The Office Action also cites col. 25, lines 64-67 and col. 26, lines 1-3, but these sections simply state that tickets may be transferred between trusted agents. This does not teach or suggest the particular features defined in claim 8.

The Office Action further states in rejecting claim 8 that X is a function of a hash, which is inherently a random number generator, hence X will always yield a unique value. However, as defined in col. 11, line 47, X is clearly disclosed to be $\text{TS}(\text{id}) || \text{TS}(\text{PK}) || \text{expire data}$, which is not a function of a hash value, and is not a random number. The Office Action also states that FIG. 6A shows that X is known to the computer of the ticket consumer since $\text{cert}(\text{TA})$ is a function of $\text{cert}(\text{TS})$ and is known to the CTA.

However, this presumes incorrectly that X is the same as cert(TS). For at least these reasons, Applicants respectfully request reconsideration and withdrawal of the rejection of claim 8 and dependent claims 9-23.

As to claim 24, Rosen fails to disclose or suggest at least that a ticket consumer's computer transmits ticket order data to a ticket provider's computer and that the ticket provider's computer receives the first transmitted ticket order data and digitally signs the ticket data. The Office Action cites col. 6, lines 7-12 and col. 12, lines 1-3, directed to validating certification of a trusted agent, for teaching this feature. However, the first transmitting according to claim 24 must be ticket order data, and the ticket data must be digitally signed. This is not met in Rosen.

Col. 6, lines 7-12 describe a digital signature of an electronic object. An electronic object in Rosen is defined as an encrypted object such as a movie, a game, etc. The digital signature of an electronic object is not stated to be from received ticket order data transmitted from the ticket consumer. Further, regarding col. 12, lines 1-3, the validation of cert(TA) and cert(TS) does not include a digital signature, from a ticket provider's computer of data provided by a ticket consumer's computer. This is because, as previously stated, cols. 11 and 12 describe a certification process only from a trusted server to a trusted agent or from a primary trusted server to a trusted server, not between trusted agents.

Additionally, regarding dependent claim 25, Rosen does not disclose or suggest that a ticket consumer's computer calculates a number R and hash(R), and that the ticket provider's computer receives the hash(R) and calculates a digital signature. Instead, the cited

disclosure of Rosen for this feature relates to a one-time certification process used before distribution of the trusted agent (CTA or MTA) to the public. Accordingly, Applicants respectfully submit that claims 24 and 25, and dependent claims 26-28 are allowable over the references of record, including Rosen. Applicants respectfully submit that claim 29 is allowable for similar reasons.

Regarding claim 30, Rosen does not disclose or suggest a digital signature of an issuer of a ticket where the medium contains $\text{Sign}(s, I || \text{hash}(R)) || R$, where R is a random number private to the ticket consumer. As claimed, $\text{hash}(R)$ is a one-way function of R and $\text{Sign}(s, I || \text{hash}(R))$ is a digital signature in respect of signature key s private to the ticket provider of the $\text{hash}(R)$ appended to information I . The Office Action relies upon a disclosure that tickets can be transferred between trusted agents, citing cols. 11 and 12. However, nothing in cols. 11 or 12 discloses or suggests that a digital signature of the issuer of the ticket (either the merchant or the MTA) is made of $\text{hash}(R)$ where R is a random number private to the ticket consumer (consumer or CTA). Similarly, Applicants respectfully submit that claim 32 is allowable. For similar reasons, Applicants respectfully submit that claim 33 is allowable over Rosen.

As to claim 34, Rosen neither teaches nor suggests at least data including a signed digital representation of a parameter generated in sequence first by the buyer of the ticket as a non-invertible function of a random number and then by the seller of the ticket as a digital signature of the first-time-made non-invertible function. Particularly, Rosen does not disclose that the digital signature of the buyer (merchant or MTA) is of a non-invertible

function of a random number produced by the buyer of the ticket (customer or CTA). Further, the Office Action submits that a non-invertible function is represented by $\text{hash}(X)$ where X represents a random number. However, as stated above, X in Rosen equals a trusted server ID concatenated with a trusted server public key, further concatenated with expiration data, and thus is not a random number. Accordingly, Applicants respectfully submit that claim 34 and dependent claims 35-37 are allowable over Rosen.

Regarding claim 49, Applicants respectfully traverse the rejection in view of Rosen for at least the reason that Rosen fails to teach or suggest at least a one-way transformation of a private number from a ticket buyer computer to a seller computer and a signing at a second time, by the ticket seller computer, this one-way transformation and additional information. The Office Action, in response to Applicants' previous remarks, states that "this has already been traversed above". However, as clearly disclosed in cols. 11 and 12 of Rosen, any one-way transformation of a number in these cited columns is of a number X or Y . Neither X nor Y is random, and both are part of a one-time initialization process between either a trusted server and a trusted agent, or between a primary trusted server and a trusted server. Thus, the relationship is not between a consumer trusted agent and a merchant trusted agent. Accordingly, Applicants respectfully traverse the rejection.

As to claim 50, the Office Action also states that "this has already been traversed above". However, as submitted regarding claim 49, Rosen neither teaches nor suggests a sending of a one-way transformation of a private number from a ticket buyer computer to a ticket seller computer and assigning at a second time the one-way

transformation and additional information to the ticket seller computer. Accordingly, Applicants respectfully request reconsideration and withdrawal of the rejection.

Claims 38-46 and 41-55 stand rejected under 35 U.S.C. §102(e) as being anticipated by Mengin. Applicants respectfully traverse the rejection. Regarding claim 38, the Office Action states, in response to Applicants' previous arguments, that "on paragraphs 51-53 the customer/ticket buyer generates a message composed of self-identifying information. This message is called digamas and it is hashed. Hashing forms a noninvertible transformation of this message/number." While claim 51 describes information forming a message, a digamas, and a hashed digamas, paragraphs 76 and 77 clearly state that the message in the "digamas" is composed by the merchant M. See, for example, paragraph 76, line 5.

Further, claim 38 also defines that the number is determined by the ticket buyer only. However, Mengin states clearly that the digamas is based on a message including particular data concatenated in a prescribed, constant order. The determination of this information forming the message is sent from the customer to the merchant in response to a query (paragraph 75, 76).

As to claim 39, the Office Action states that the feature wherein the communication channel is sending at the second time a random number is met on paragraph 20 of Mengin. However, paragraph 20 describes a linking of a random number uniquely associated to a sample of paper. This random number does not appear to be related to the generation of the number (or digamas), the message, or a digital signature as defined in claim

38. Instead, this random number is a number associated reproducibly with a random sample of material obtained only by at least one of chemical and physical processes, and then by including that number into an area of the object. The random number is uniquely associated to the sample of paper where the document is printed. This is a separate aspect of the description of Mengin. See, for example, paragraphs 17 and 18 (describing a first aspect and a second aspect, respectively).

As further described in paragraph 18 of Mengin, the random number used in the second aspect of the invention is associated with the sample by using a specific reader, and does not appear to be related to a number determined by the ticket buyer only. If such a number is used in a digamas (paragraph 101), this number would likely be determined by the ticket seller (to prevent reproduction of the ticket by the ticket buyer), and not by the ticket buyer only, as defined in claim 38. Accordingly, Applicants respectfully submit that claim 38 and dependent claims 39-44 are allowable over the references of record, including Mengin.

As to claim 45, the Office Action states that the feature of a 2-D bar code indicia containing a one-way function of a number provided by a holder of the ticket is met in paragraphs 53-55 of Mengin. However, in Mengin, the one-way function (i.e. the hashed digamas) is of a number (digamas) provided by the merchant, not a holder of the ticket, as clearly disclosed in paragraphs 75 and 76, as well as paragraph 17. Though, as the Office Action states, the message is composed of self-identifying information, this information is first provided to the merchant, and the merchant converts this information to a message, e.g., by concatenating the information in a prescribed, constant order (paragraph 51). The

merchant, not the ticket holder, then reinterprets this formed message into a digamas. Accordingly, Applicants respectfully submit that claim 45 and dependent claim 46 are allowable over Mengin.

As to claim 51, the Office Action states in response to Applicants' previous remarks that "the limitation argued by the attorney is not contained within claim 51 limitation". Thus, to clarify, Applicants respectfully submit that Mengin fails to disclose or suggest at least sending from the computer of a ticket buyer (not seller, as was submitted in error), to the computer of the ticket seller (not buyer) second data accompanied by a secure first transformation of the number that is determined by the ticket buyer only and unknown to others including the ticket seller.

As clearly stated in paragraphs 51-55, a message is concatenated, by the merchant in Mengin, in a prescribed constant order, and is reinterpreted digitally, again by the merchant, to form a number called a digamas. Because the ticket seller, i.e., the ticket merchant, is stated to prepare this number (paragraphs 51-53, paragraph 17) this number is clearly known by the merchant. This is contrary to the defined feature in claim 51 in which the number is determined by the ticket buyer only and unknown to others including the ticket seller. Accordingly, Applicants respectfully submit that claim 51 and dependent claims 52-55 are allowable over the references of record including Mengin.

Claim 48 stands rejected under 35 U.S.C. §103(a) as being unpatentable over Mengin in view of Rosen. Applicants respectfully traverse the rejection for at least the reasons stated above regarding Rosen and the claimed feature of a number $\text{Sign}(\|\text{hash}(R)\|)$.

Additionally, neither Mengin nor Rosen teaches that R is a number having its origin in a computer of a consumer of a ticket. Also, Mengin does not teach or suggest that the number R is private to the ticket consumer, as stated above. Applicants thus respectfully request reconsideration and withdrawal of the rejection.

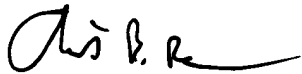
For at least the foregoing reasons, Applicants believe that this case is in condition for allowance, which is respectfully requested. The Examiner should call Applicants' attorney if an interview would expedite prosecution.

Respectfully submitted,
GREER, BURNS & CRAIN, LTD.

Customer No. 24978

March 24, 2005

300 South Wacker Drive
Suite 2500
Chicago, Illinois 60606
Telephone: (312) 360-0080
Facsimile: (312) 360-9315
P:\DOCS\0321\67683\802774.DOC

By: 
Arik B. Ranson
Registration No. 43,874